Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6504
Transmittal Sheet
June 7, 2006

RESTRICTIONS ON TRANSMISSION, TRANSPORTATION AND USE OF, AND ACCESS TO, VA DATA OUTSIDE VA FACILITIES

1. **REASON FOR ISSUE:** To provide Department of Veterans Affairs (VA) policy regarding transmission, transportation and use of, and access to, VA data outside VA facilities.

2. **SUMMARY OF CONTENTS:**

   a. This directive sets forth restrictions applicable to VA employees' transmission, transportation and use of, and access to, VA data while working in locations other than a VA facility. It describes required security measures for mobile or fixed computers, other electronic and storage media used to transmit, transport, process, store, or access information or connect to VA IT systems from home, on travel, or at alternative work locations. It also restricts the use of VA data stored in non-electronic form outside the regular work site.

   b. Employees have no right to transport, transmit, use or access VA data outside the regular work site except as set forth in, and in accordance with, this Directive. VA Administrations and Staff Offices will establish necessary controls to ensure that the data is handled securely and appropriately.

   c. This directive does not supersede any other applicable law or higher level Government-wide policy guidance, but does supersede any other inconsistent Department, Administration or Staff Office policy, or policy sections, that deal specifically or generally with employees' transportation, transmission, use of, or access to, VA data outside VA facilities.

3. **RESPONSIBLE OFFICE:** The Office of Cyber and Information Security (005S) in the Office of Information and Technology (005) is responsible for the material contained in this directive.

4. **RELATED HANDBOOK: None**.

5. **RESCISSION:** Office of Cyber and Information Security (005S) Security Guideline for Single-User Remote Access, Revision 3.0, dated March 10, 2006.

CERTIFIED BY:

/s/
Robert T. Howard
Senior Advisor to the Deputy Secretary
Supervisor, Office of Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Gordon Mansfield
Deputy Secretary

RESTRICTIONS ON TRANSMISSION, TRANSPORTATION AND USE OF, AND ACCESS TO, VA DATA OUTSIDE VA FACILITIES

1. PURPOSE AND SCOPE. This Directive establishes policy and responsibilities for VA employees' transmission, transportation, and use of, and access to, VA data outside VA facilities. This Directive applies to all VA organizational elements, and all VA employees.

2. POLICY0.

a. General. VA employees are permitted to transport, transmit, access and use VA data outside VA facilities only when such activities have been specifically approved by the employee's supervisor and where appropriate security measures are taken to ensure that VA information and services are not compromised. The privilege to use or access VA data outside VA facilities may be revoked or limited at any time by appropriate VA Administration and Staff Office officials.

b. VAGFE and OE. Only VA-owned Government Furnished Equipment (VAGFE), including laptops and handheld computers, may be used when accessing the VA intranet remotely. VA employees may not use non-VA owned Other Equipment (OE) to access the VA intranet remotely or to process VA Protected Information (VAPI) except as specifically provided in this Directive. VAPI is sensitive information as defined in paragraph 5 titled "Definitions." Access to the VA Intranet using non-VA owned Other Equipment (OE) will be provided via approved VA Virtual Private Network (VPN) access protocols, which will offer access to a limited set of VA applications and services. Only remote access users with VAGFE will be permitted to connect to the VPN in such a way that grants full VA access provided all required security software is installed and updated.

c. Initiation and Termination of Remote Access Accounts. Employees must request and obtain supervisory approval for remote access to the VA Intranet. The employee or supervisor may apply for a remote access account through the Information Security Officer (ISO).

(1) Remote access accounts are as-needed accounts. Unused accounts must be disabled and removed if no longer needed. If a remote access account is not used for a period of ninety (90) days, the ISO will disable the account. If a remote access account remains unused after six months, the ISO will remove the account. If the account is deleted and remote access is subsequently required, the employee must request a new account.

(2) Supervisors will ensure that remote access privileges are terminated as soon as they are no longer needed, when the account owner transfers out of the supervisor's office or leaves the VA, or when an authorized official determines that remote access privileges should be revoked. Upon termination of required access privileges, supervisors will confirm and notify the ISO that the employee has returned all VAGFE related to remote access.

d. System Security. Only VA personnel may access VA-owned equipment used to process VA information or access VA processing services. Employees may not share with non-VA employees or unauthorized personnel instruction or information regarding how to establish connections with VA private networks and computers. Employees may not share remote access logon IDs, passwords, and other authentication means used specifically to protect VA information or access techniques to VA private networks.

e. Operating System Controls. Employees must use only computers and electronic storage media configured to conform with **all** VA security and configuration policies to store, transport, transmit, use and access VAPI.

(1) Required for both VAGFE and OE:

(a) VA employees must use passwords that meet VA password requirements.

(b) The "save password" feature must not be used for passwords that provide access to the operating system or VA network services

(c) "Blank" and default user names and passwords must not be used

(d) User credentials including passwords are considered VA sensitive information and must be protected appropriately

(e) A shared file or drive containing VAPI must not be created on a device used for remote computing. File sharing of VAPI must only be accomplished through the use of authorized VA servers.

(f) VAPI or VA-specific software must be segregated in dedicated directories that are protected

(g) If VAPI such as Protected Health Information (PHI), privacy information, or information that could be used by unauthorized persons to gain access to VA systems is to be stored outside of the VA intranet or outside of the physical protection of VA facilities, it must be protected. (See the *Data Handling* section.)

(2) Required for VAGFE and for OE used to access or process PHI or other VAPI.

(a) Password-protected screensavers must be configured to activate after five minutes of inactivity.

(b) The screen saver must be activated manually when the workstation is unattended.

(c) Anti-virus software must be installed and operational (refer to paragraph g below).

(e) All devices must conform to operating system hardening guidelines as specified in VA Information Security guidance.

f. Protection from Viruses and Other Malicious Code. Certain protection mechanisms are required to protect systems connecting to the VA intranet and/or containing VAPI against viruses and other malicious code.

(1) VAGFE and OE that contain VAPI must be equipped with, and use, a VA-approved antivirus (AV) software and a personal ("host-based") firewall that is configured with a VA-approved configuration.

(2) In the event that the computer/device connecting remotely is simultaneously attached to a second network (such as an in-home LAN), either the secondary network computers/devices must be provided with similar AV and host-based/personal firewall protection, or all other connections must be severed.

(3) VAGFE devices attempting to access the VA intranet remotely via the One-VA VPN client must have the AV and Host-based Intrusion Prevention System (HIPS) software installed and current, including all critical updates and patches, in order to be granted access to the VA intranet. HIPS software must also be installed and current, including critical updates and patches, on non-VA OE that will connect via the One-VA SSL VPN option before such OE may be used to transport, transmit, access, process or store VAPI. For additional information regarding software required for use on VAGFE or recommended for use on OE, refer to the document titled *"Anti-Virus/Firewall accepted for use on non-government owned equipment attached to the One-VA VPN." (This document may be found on the Office of Cyber and Information Security intranet web site.)*

g. Antivirus Software. VAGFE and OE used to transmit, transport, access, process or store VAPI must be equipped with current, VA-approved anti-virus software. The local facility Information Resource Management (IRM) Office or local ISO will provide the software for VAGFE. Employees using non-VA OE devices to access the VA intranet remotely must comply with the policy set forth in "*Anti-Virus/Firewall accepted for use on non-government owned equipment attached to the One-VA VPN*." If non-VA OE is connected to a home or small office network with other workstations, all interconnected workstations must have virus protection. Anti-virus software must contain a real-time scanning feature, which must be enabled. Employees must update their antivirus software and check for viruses before use of any diskette or file they encounter that is of uncertain or unauthorized origin. Data and executables copied from removable media, the internet, or email must be scanned for viruses as soon as reasonably possible after their introduction on the computer. Executables must not be launched without first having the origin validated by the sender and verified to be free of viruses.

h. Host-based Intrusion Protection System/Personal Firewall. Employees using VAGFE to access the VA intranet remotely must use the HIPS provided as part of the One-VA VPN client solution. Employees using non-VA OE devices to access the VA intranet remotely must comply with the policy set forth in "*Anti-Virus/Firewall accepted for use on non-government owned equipment attached to the One-VA VPN*."

i. Enclave/Perimeter Firewalls. Any employee who uses a computer to connect to the internet outside the regular work site, whether VAGFE or non-VA OE, must ensure that the computer is protected by a firewall. The firewall may be enclave-based or host-based. The boundary between a user and the Internet is considered an enclave perimeter with the user residing in the enclave. Any firewall software and/or firmware must be maintained at the most current release and patch level and configured separately. This includes personal/home use internet routers such as those produced by Linksys/Cisco, D-Link, Netgear, etc., and those used to protect other permanent connections such as Local Area Networks (LANs) of small offices, facilities, etc.

j. Application Software Security. Users with NT, W2K, and systems administration capability must scan their system for vulnerabilities. Those dependent on third-party system administration must arrange to have their systems updated regularly.

k. Virus or Malicious Code Infection Handling. Employees must immediately stop using any computer or software suspected of malicious infection or malfunction. In all such cases, the machine must be immediately isolated from any VA network connections. Do not reboot (turn off/on) the system, as many viruses are triggered to propagate upon system reboot which can cause further damage. If it appears that a negative activity is occurring (such as the deletion of files) then the system must be shut off and left off until a clean Antivirus boot media is used to clean the system. Employees not authorized to attempt recovery and restoration must not remove the suspected software themselves, but must contact a qualified IT Specialist via their respective help desks to attempt recovery. Recovery must be attempted only by an authorized IT Specialist. If a non-VA technician is called to service non-VA OE, the employee must exercise caution to protect VA data, including information that facilitates access to VA private networks. An employee must never surrender or swap hard drives or other storage to an outside party if he or she was storing VAPI at the time of the system problem. Only VA-approved software and tools may be used to attempt recovery from virus or other malicious code infection.

l. Remote Access Configuration. Only VA-approved remote access solutions may be used. All remote connections to VA networks must be through OCIS-authorized configurations and access points. No VA employee is authorized to use VA remote access services to engage in any activity that is illegal or violates VA policies. While connected to VAGFE, do not simultaneously connect to VA and one or more non-VA networks. VPN client software must not be configured to support split or dual tunneling, which allows the user's computer to connect to the VA while simultaneously connected to another public network such as the Internet. Inactive sessions must be terminated by logging off when finished or when leaving the workstation unattended. Employees must not turn off the device or monitor without first logging off. All VAGFE are required to have a password-protected screensaver enabled.

m. Remote Access Via Non-VA Networks. Non-VA networks refer to third-party networks that are considered "untrusted" by the VA. The One-VA VPN gateway, which includes both the IPSec and SSL VPN devices, is the VA's method for securely using non-VA network services to access VA networks. Third-party, untrusted network examples include: dial-up or broadband access to an Internet Service Provider (ISP), visiting a non-VA network, and wireless connections. VA-approved VPN software and/or hardware are required to create VPN or Extranet connections to VA private networks.

n. Remote Access Using Wireless Networks Wireless routers and access points, even if not used at the enclave perimeter, must be configured in accordance with the "*VA Wireless and Handheld Device Security Guideline.*"

o. Data Handling. VA Staff Offices and Administrations must conduct risk assessments and Privacy Impact Assessments as specified in applicable VA policy, and protect VAPI in compliance with the results of the risk and Privacy Impact Assessments.

p. Protection Of Information. VA information may not reside on non-VA system or devices unless specifically designated and approved in advance by the appropriate VA official (supervisor), and only where the non-VA systems or devices conform to, or exceed, applicable VA security policies or are specifically authorized by VA guidance.

(1) VAPI must not be transmitted by remote access unless VA-approved protection mechanisms are used. All encryption modules used to protect VA data must be **validated** by NIST to meet the currently applicable version of Federal Information Processing Standards (FIPS) 140 (See http://csrc.nist.gov/cryptval/140-1/1401val.htm for a complete list of validated cryptographic modules). Only approved encryption solutions using validated modules may be used when protecting data during transmission.

(2) Passwords or other authentication information must not be stored on remote systems unless encrypted. VA-PKI certificates must be stored in encrypted form only and must be accessible only by using a personal identification number (PIN) or password.

q. Data Stored – Encryption. Additional security controls are required to guard VAPI stored on computers used outside VA facilities. If an employee uses VAGFE or non-VA OE in a mobile environment (e.g. laptop or PDA carried out of a VA office or a PC in an alternative work site) and VAPI is stored on the computer, file or electronic storage media, approved encryption software must be used. The file or hard drive encryption software must be FIPS 140 certified, operated in FIPS 140 mode and all VAPI stored on the computer must be stored in the encrypted partition created by the encryption application. The application must be capable of key recovery and a copy of the encryption key(s) must be stored in multiple safe locations with the supervisor and ISO.

r. Backup. A remote or mobile computer must not contain the only copy of VA records or data. Employees must make redundant copies ("backups") of essential business data and software at regular intervals. Employees must store multiple sets of backup data in protected locations other than the location of the device containing the data. Back-ups and archives must be treated according to their VA security classification.

s. Theft, Loss, or Compromise. If an employee becomes aware of the theft, loss or compromise of any VAGFE or non-VA OE device used to transport, access or store VA information, or of the theft, loss or compromise of any VAPI, the employee must immediately report the incident to his or her supervisor and the local ISO. The ISO will promptly determine whether the incident warrants escalation, and comply with the escalation requirements in "Responding to Security Incidents and Malfunctions."

t. Hard-Copy Documents and Physical Media. VA personnel are responsible for ensuring that VAPI, in hard-copy documents or on physical media, under their control, is protected from improper disclosure, including inadvertent disclosure. When no longer needed, VA information classified as VA sensitive must be destroyed by a method rendering it unreadable, undecipherable, and irretrievable as prescribed in the most current version of "Fixed Media Sanitization" (see paragraph 4.b.(12) below) and its attachment.

u. Physical Security. The following rules are applicable to all VAGFE and non-VA OE used to transmit, transport, access, process or store VA data:

(1) Equipment, information, or software must not be taken off-site without express authorization by the employee's supervisor.

(2) Equipment must be housed and protected to reduce the risks from environmental threats and hazards, and the opportunities for unauthorized access, use, or removal.

(3) Portable computers that have VAPI on their storage device(s) or have software that provides access to VA private networks must be secured under lock and key when not in the immediate vicinity of the responsible employee. This includes external hard drives and other storage devices. If such devices are maintained in a hotel room or residence, they must be stored out of sight and the door(s) to the room or residence must be locked when the employee is not physically present.

(4) Employees must use physical locks to secure portable computers to immovable objects when the computers must be left in a meeting room, or other semi-public area to which individuals other than the authorized employee have access.

(5) When in an uncontrolled environment, employees must follow "clear desk" [define] practices for media to reduce the risk of unauthorized access to, loss of, and damage to VAPI. No VAPI may be left on desks.

(6) When in an uncontrolled environment (for example, when traveling on an airplane or in an airport), employees must guard against disclosure of VAPI information through eavesdropping, overhearing or overlooking (shoulder surfing) by unauthorized persons. When traveling, employees must keep portable computers or storage devices in their possession, and may not check them as baggage.

(7) Data and system backups that include VA information have the same confidentiality classification as the originals. Therefore, these materials must be protected with the same or equally effective physical security as that provided to the source computer, its media, and information contained therein.

(8) Backups must be stored where they are physically secured yet accessible within a reasonable time frame when they are needed in accordance with applicable VA policy.

v. Sanitization. Any VA employee who uses OE to transmit, transport, use or access VAPI must sanitize the OE device to remove the VAPI when the employee is no longer using the device to perform VA work or when the device is not compliant with this Directive. Sanitization must be done in accordance with the most current version of "Fixed Media Sanitization" (see paragraph 4.b.(12) below) and its attachment.

w. Waiver. No waiver to any requirement of this Directive may be granted except by request of an Administration Head, Assistant Secretary or other Key Official to the CIO.

3. RESPONSIBILITIES:

a. VA OCIS. OCIS is responsible for developing appropriate technical standards and guidance for the use of computers and other devices to transport, transmit, access, process and store VA data outside the regular work site. OCIS is also responsible for identifying approved

monitoring mechanisms to confirm compliance with this policy; reviewing remote access technology standards and procedures periodically with security personnel, verifying compliance for Certification and Accreditation; supporting risk management activities associated with business and network operations; acting as the central coordination point and final approval authority for exceptions to this policy; defining or approving acceptable methods of remotely connecting to the VA systems; and providing immediate consultation to VA administrations.

b. VA Chief Information Officer (CIO). The CIO is responsible for assuring Department-wide adherence to current VA network security policies, directives and standards; developing and implementing supporting procedures to confirm conformance with VA network security and remote access policy and standards; operating in a secure manner, commensurate with their security sensitivity, common security services for use by applications and other infrastructure services; examining systems to validate remote access requirements, ensure proper systems configuration, detect unauthorized remote access connections, report violations, and confirm that appropriate security mechanisms and monitoring devices are up to date with best practices and technical standards; supporting risk assessment activities and support technical and security standards for remote access; approving individual requests for remote access based on business requirements, including restrictions and limitations that should be applied; providing operational training for remote access; preparing and providing security and awareness training for all users; defining procedures for remote administration and troubleshooting; maintaining and reviewing an inventory of all remote access users; and maintaining audit logs in accordance with certification and accreditation requirements.

c. All VA Employees. Employees who transport, transmit, access, use, process or store VAPI outside VA facilities (even once) are responsible for requesting and obtaining supervisor and ISO approval for such transport, transmission, access, use, processing or storage; reading and following the remote access security policies; accessing only information systems that use approved hardware, software, solutions, and connections;; taking appropriate measures to protect information, network access, passwords, and equipment; refraining from using automatic password saving features; using extreme caution when accessing VA information in open areas or areas where non-authorized persons may see VA information such as airport lounges and hotel lobbies; protecting VA equipment and information from loss or theft at all times, especially when traveling; exercising good judgment in the use of these resources; complying with current and future standards of acceptable use and conduct at all times; and promptly reporting any misuse of the remote access process observed or possible compromise or loss of VAPI.

d. Information Security Officer (ISOs). ISOs are responsible for coordinating and documenting all requests for remote access within their region, facility or facilities; enforcing all policies and procedures pertaining to transportation, transmission, remote access and use of VA IT equipment; monitoring remote access account usage and ensuring dormant accounts are disabled or removed per this Directive or local policy where more restrictive; ensuring that remote access accounts are immediately disabled for all persons no longer requiring remote access; ensuring that all VA IT equipment used for remote access and VA data storage is immediately retrieved and processed according to policy; and working with the VA-SOC to ensure that remote access to the VA network is done only via approved and appropriately documented methods.

4. REFERENCES

a. Federal Standards

(1) Federal Information Processing Standard (FIPS) 140-2, *Security requirements for Cryptographic Modules*

(2) Draft NIST Special Publication 800-77, *Guide to IPSec VPNs*

(3) NIST Special Publication 800-61, *Computer Incident Handling Guide*

(4) NSA/CSS Manual 130-2, Media Declassification and Destruction, Nov 2003

(5) DoD Hard Disk Sanitizing Guidance, DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*

b. VA Policies, Directives, and Security Configuration Guidelines

(1) You and Your Password, August 15, 2005

(2) HISD-MDHG-pcAnywhere 11.5 V2.2 (2)

(3) *VA Security Configuration Guideline For Symantec pcAnywhere Version 11.5 Draft Revision 1.1, Feb 28, 2005*

PC AnywhereConfigurationGuidelinev1.1.doc

(4) *VA Security Configuration Guideline For Danware NetOp Remote Control Version 7.6, February 17, 2004 (Contact TIS)*

(5) *VA Security Configuration Guideline For DameWare NT Utilities & DameWare Mini Remote Control, Version 2.1 (Draft), August 20, 2005 (Contact TIS)*

(6) VA Memo, Limitations of the Installation of Modems in Desktop Computers, 15 November 2004

(7) VA Directive 6212, Security of External Electronic Connections

(8) VA Memo, *Unsecure Dialin,* Oct 13, 2000

(9) VA Memo, VPN within the VA Enterprise, July 18, 2003,

(10) *Information Systems Security Incident Reporting VHA Security Policy Procedures Template, Version 1.0, Aug 2004,*

(11) *Anti-Virus/Firewall accepted for use on non-government owned equipment attached to the One-VA VPN, 5 May 2005,*

(12) VA Memo, Fixed Media Sanitization, April 20, 2004,

(13) VA Wireless and Handheld Device Security Guideline, Version 3.2, August 15, 2005

(14) VA Handbook 5011/5, Hours of Duty and Leave

5. DEFINITIONS

a. Alternative work location. For the purposes of information security, an "alternate work location" is any place where VA personnel are performing VA work while outside a VA managed facility, or when remote computing is the only means of access (for example, a small department office with only dial-in access). Examples include residences and hotel rooms.

b. Asset. Property of VA or another government agency such as personnel, hardware, software, data and facilities.

c. Availability – making sure that information and vital services are available to users when required.

d. Classification. The assignment of information or an information asset to categories on the basis of the information's need for confidentiality, integrity, and availability.

e. Controllable Environment. Inside VA office buildings and other VA facilities were the security risks have been recognized and control can be exerted on work guidance.

f. Confidentiality. Protecting information from unauthorized disclosure or intelligible interception.

g. Host-based/Personal Firewall. A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are used frequently to prevent unauthorized Internet users from accessing private systems or networks connected to the Internet. All messages entering or leaving the remote computer or network pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

h. Information Assets. Information, information systems, information services, and information processing resources owned by or entrusted to the VA. Information can exist in several forms (written, verbal, physical, and electronic) and in various states (static or transient).

i. Information Processing Resources. The collection of equipment, software, network connections, and applications and the processes they support to handle data to derive and convey information.

j. Information Security. Protection of information to ensure its Confidentiality, Integrity, and Availability.

k. Integrity – Safeguarding the accuracy and completeness of information and computer software and services.

l. Mobile Computing Device. Any transportable computing or storage device to include personal digital assistants (PDAs), notebooks, desktops, servers, and mobile telephones.

m. OE. Non-VA owned equipment, including employees' personal equipment, commercial equipment (such as hotel and internet café equipment), and equipment owned by other agencies.

n. PAI. Privacy Act Information – information covered by and protected under the Privacy Act of 1974.

o. PDA. Personal Digital Assistant. Describes a class of handheld computing devices (Palm, Pocket PC, etc.) designed to serve the mobile computing needs of individuals. Applications delivered with PDA hardware include email, calendar events, contacts, and PC synchronization.

p. PHI. Protected Health Information. Information protected by the HIPAA Privacy and Security Rules, 45 CFR Parts 160 and 164.

q. PKI. Public Key Infrastructure. PKI is an environment based on the use of digital certificates and public and private key technology to secure communication of information. A fully deployed PKI supports encryption, authentication, privacy, and non-repudiation of information.

r. Remote. An adjective used to describe the use or processing of, or access to, VA information from locations other than sites in VA facilities.

s. Security Incident. An event that has, or could have, resulted in loss or damage to VA assets, or an action that breaches VA security procedures.

t. Telecommuting or Telework. (Performing VA work at a work location other than one directly maintained by the Department, including work done at home. In the context of security, the term applies equally to work performed while traveling on VA business or when at a customer's or vendor's site.

u. Uncontrollable Environment. Locations other than in VA facilities.

v. VA Data or VA Information. All information that is obtained, developed, or produced by or for VA or its employees as part of its business activities.

w. VAPI. VA Protected Information. VA sensitive information, Privacy Act Information (PAI), PHI, or other VA information that has not been deliberately classified as public information for public distribution. VA information that VA would have to release under the Freedom of Information Act is not VA Protected Information. All VA Protected Information should be classified as one of the following: VA Proprietary, VA Restricted, or VA Highly Restricted.

x. VA Sensitive Information. VA sensitive information is all Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of federal programs.